ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/346049815

An Approach to Musical Cryptography

Conference Paper · November 2020

CITATIONS
0

READS
4,006

2 authors:

Tannisha Kundu
Amity University
13 PUBLICATIONS **14** CITATIONS
SEE PROFILE

Anurag Sinha
Amity University Jharkhand
141 PUBLICATIONS **553** CITATIONS
SEE PROFILE

All content following this page was uploaded by Anurag Sinha on 21 November 2020.

The user has requested enhancement of the downloaded file.

IWCSET20-CSE-048 ISBN: 978-93-5407-648-0

An Approach to Musical Cryptography

Anurag Sinha Tannisha Kundu

Department of computer science, Scholar, Amity University Jharkhand

Ranchi, Jharkhand(India), 834001

Department of computer science, Assistant Professor, Amity University Jharkhand

Ranchi, Jharkhand(India), 834001

anuragsinha257@gmail.com[1]

tkundu@rnc.amity.edu[2]

ABSTRACT- ***The craft of scrambling messages utilizing music is named as Musical cryptography and it utilizes predefined set of notes and set of rules for making melodic pieces which thus are melodic cryptograms. Traditional methodologies applied to melodic cryptography utilized basic replacement figure which produces melodic arrangements. - Music and its trademark have been utilized in various region of world. Music can be utilized as a language of correspondence. Music notes have been utilized in the field of transcription and cryptography in early days. A part of information is covered up inside a melodic note and ships off the objective. Melodic images and melodic notes have been utilized as the replacement figure. The fundamental objective of the melodic cryptography is to produce distinctive melodic cryptograms. Any melodic note comprises of seven fundamental keys. Our ordinary Indian music is made of the seven keys Sa, Re, Ga, Ma, Pa, Dha, Ni. The western music notes depend on the seven keys C, D, E, F, G, A, B. Utilizing these notes as the fundamental notes, music is created. Utilization of music notes in encoding any message isn't in wide use. In this paper we propose a strategy for encryption of any instant message utilizing the Indian and western music notes.***

Keywords— Musical Cryptography,indian ragas, music sheet cipher, guitar chords encryption, genetic algorithm

1.INTRODUCTION

In this period of innovation, with the utilization of Internet and its different advances our customary correspondence has been changed into computerized correspondence. In this computerized period, keeping message mystery is a fundamental issue to be tended to. To manage with this test cryptography is utilized in data security. The messages rather data to be sent to target by and large we individuals utilize explicit language for the transmission. Their objective is any individual who doesn't perceive the snippet of data they stow away. The message to be communicated is commonly called as plain instant message. Cryptography is the specialty of changing the content or information into a coded plan or some other encoded structure.

A cryptographic methodology is trailed by two calculation: encryption Algorithm for encoding the information into progressive coded design and an unscrambling calculation which remodels the coded message into its certified message. The center objective of cryptography approach is to apply changes to the plain content and with the end goal that the message not, at this point remain behinds usable to an interloper without applying the nullify change.

Cryptography known to be is the investigation of techniques for sending messages in jugglery structure so just the planned beneficiaries can peruse the message. The message we need to send is known as the plaintext and the disguised message is known as the code text. Maintaining privacy and covering messages have picked up essentialness directly from the earliest starting point of progress. As and when a picky strategy for encryption becomes well known, the risk of cryptanalysis increments and consequently new procedure should be imagined or distinguished to give the expectation.

Contingent upon the key used to encode and unscramble the code calculations are delegated symmetric key and lopsided key calculations. Symmetric key calculations utilize the indistinguishable key for encryption and unscrambling measure. Awry Key calculation utilizes generally unique key for encryption and unscrambling. Symmetric Key is otherwise called private key cryptography a mystery key is being have similar feeling upon previous exchange of messages, contingent upon the key the sender side scrambles the message and beneficiary side decodes the message. In this paper, Musical cryptography ideas convert the plain instant message into melodic notes or melodic images. In melodic cryptography music and its credits to encode the plain content into its comparing figure text. The code messages can be emblematic, verbal or instrumental notes.

2. RELATED WORK

Musical notes and the alphabet are together tools for communication. Music uses 12 tones, while the English alphabet uses 26 letters. Numerous mappings of music notes to the alphabet can alleviate the encryption plaintext into music cipher text. Musical symbols have been used in cryptography from the earliest times. As a subject of fact, a number of cryptologists were also famous musicians. Faber, Haydn, Bach, Schumann are examples of composers who embedded "cipher themes" in their work. For these artists, musical masterpiece with cipher techniques was a mere method to raise the value of their work. While the cryptographic value of their efforts was somewhat limited, their practice derives from awareness that music and semantics have commonalities.

The idea of replacing plaintext characters with musical notes may engage musical notes in the form of visual succession (musical symbols/notations), vocal or instrumental music. The present paper is mainly concerned with plain text characters encrypted as sequence of musical notes from an instrument. The challenging part in designing a music cryptographic method is to come up with an suitable mapping of plain text characters to musical notes so that the final musical series generated is a valid one. Strength of a musical sequence is decided based on how pleasing and tuneful it sounds, to a listener.

3. LITERATURE SURVEY

While the current studies in the area of combining music and cryptography is somewhat limited, more than a few proposals [3,7,6] in musical cryptography have involved symmetric key encryption, substitution ciphers, and stenography .

Dutta et al. [3] proposed a symmetric key algorithm for musical cryptography. The algorithm renovates plain text into a musical piece by substituting the text characters with mathematically generated musical notes. The sequence of musical notes generated for a fastidious character progression of plain text apes a musical pattern. This example is then send to the receiver as a music file. The beginning value for encryption and decryption key is sent using the RSA algorithm, where the key plots the letters equivalent to a musical note. Their encryption key used is an n x n matrix and it will be generated using the seed value for the key.

History says that many of the cryptologists have been good musicians. Also, prominent composers like Schumann, Michael Haydn, Elgar and Tartini were known to be interested in cryptography. In fact, the grounds of music and cryptography have positive correlation. The connection was also known to and used by the British wartime crypto-analytic service [19]. Earliest forms of music cryptography made use of the straightforward technique of replacing characters of the plaintext with musical symbols. Edward Elgar, a notable composer wrote a letter to Miss Dora Penny in encrypted form which is famous as "Dorabella" Cipher [6]. Bach, another musician regularly employed the natural order number alphabet (A=1 to Z=24) in his work.

Considerable quantity of effort has been done in the pasture of music cryptography in recent years too. [4] proposed a scheme to encrypt plaintext characters encompasses English letters as well as digits 0-9 by arbitrarily assigning every plaintext character to a number between 12 and 23, which in turn represent 36 different music notes.[5] described a method that took 12 notes and 6 octaves, generating 72 music notes which can be used to reinstate plaintext characters. This process made use of a conversion table and note transition algorithm in order to denote the mapping of plaintext characters to music notes. A method to encrypt binary strings using concepts of graph theory and propagating cipher block chaining (PCBC) mode of encryption was discussed by [23]. Each string of three bits was mapped to a music note. One such 3-bit combinations corresponds to a pause/blank in the music clip. In [16], a method that used the concepts of magic-square and Polybius cipher techniques was explained. A 6X6 magic square was selected and all English letters and 0-9 digits were placed in each of its cells. Each column and each row of this magic square was labelled with C,D,E,F,G,A. Each plaintext character was thus replaced by its corresponding row column index in the magic square. Space character was replaced by the music note B. Two more methods to encrypt binary strings were discussed in [24]. in cooperation these methods considered two binary strings (one of which was the plaintext string to be encrypted) and interleave one of them into the other at specific locations in order to generate a third string. Groups of bits in that final string were mapped to different music notes. [11] proposed a method of music cryptography that made use of genesis rules and the concept of raga in Indian classical music. It was based on replacing each plaintext character with a swara from a specified raga depending on the probability of its occurrence in that raga. A method making use of a fuzzy logic was explained in [13]. This made use of various constraints like melodic rules, harmonic rules, rhythm rule, etc in order to generate multiple music clips corresponding to a text message. After that, fuzzy rules were applied and the music clip with best possible musical succession was selected and converted to a MIDI file before sending to the receiver. In [12], a combination of Play air cipher and Polybius cipher techniques was used for encryption. Initially plaintext was encrypted using Play air cipher. The encrypted message was re-encrypted using Polybius cipher. A variation algorithm was used to produce the key matrix which was used to map the text characters to parallel music notes.[14] proposed an encryption method that generated a cipher key which put up with the principles of music theory. Dissonance and uneven

 ISBN: 978-93-5407-648-0

beats were shun by creating a key that stayed in one key signature in the context of a single major level.

4. MUSIC THEORY

Scale

The most basic of all scales is a solo octave of the C major scale. This scale consists of no pointed or smooth, and can be played by basically pressing every white key on a piano from one C to the next C an octave above it. In the scale, there are seven tones which are noted as C, D, E, F, G, A, and B. The basic structure of any scale is an accretion of whole steps and half steps.

Rhythm

There are a few significant types of basic rhythms that we mention in our study. Each character in the simple replacement cipher will get one full beat of the measure or bar. Beat division is a major way of differentiating notes. There are innumerable ways to divide a single beat, but most of it can be explained through fraction.

Chords

A chord is created by playing more than 2 notes simultaneously. All chords build of a certain tonic will carry the key mark of the tonic, unless otherwise notated with inadvertent. An accidental is a sharp or level outside of the key signature used inside the notation of the piece.

Circle of fifths

The circle of fifths is normally read with C major as a preliminary point. Note G is the central or fifth in the C major scale, therefore, it is the next major scale comprised in the circle of fifths. Note D is the dominant in the G major scale, therefore it comes after G in the circle, and so on. In the key of C however, D is the second degree.

The sample of the circle goes from the first to the fifth to the ninth to the thirteenth, and so on, pending the circle is complete. Any scale degree greater than seven can be decreased by seven to attain their scale assignment in a more understandable format, thus creating a circle that goes from the first to the fifth to the second to the sixth until the circle is complete.

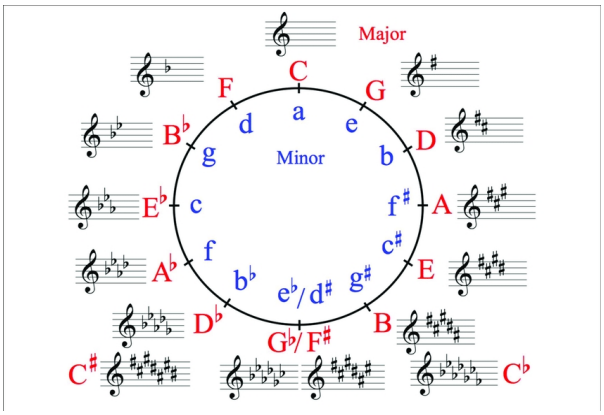


Figure 1 - circle of fifth

5. PROPOSED APPROACH

5.1 In this section we provide a brief introduction to Indian music notation and keyboard notation.[20]

Keyboard notation

Musical notation is the depiction of sound with symbols. Any music can be characterized using these symbols. The fundamental notes in music are C, D, E, F, G, A and B. A pause in music is represented by -. The following illustration signify the musical notation from C to B

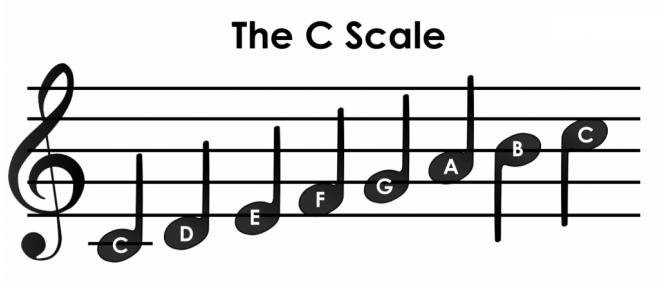


Figure - 2

Indian Musical Notation:

The seven music notes in Indian music note are known as Sudda Swar Sa Re Ga Ma Pa Da Ni. The similarity of Indian music note to the key board is shown below-

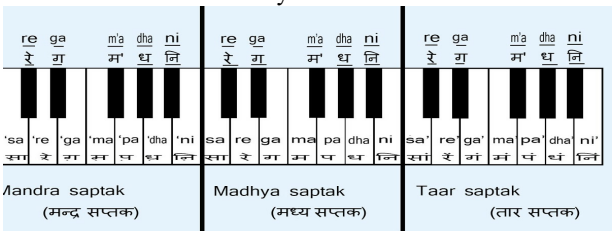

re ga m'a dha ni
रे ग म' ध नि
'sa 're 'ga 'ma 'pa 'dha 'ni
सां रें गं मं पं धं निं
sa re ga ma pa dha ni
सा रे ग म प ध नि
sa' re' ga' ma' pa' dha' ni'
Mandra saptak
(मन्द्र सप्तक)
Madhya saptak
(मध्य सप्तक)
Taar saptak
(तार सप्तक)

Figure – 3

ISBN: 978-93-5407-648-0

Encryption method

Here we propose a technique of encryption of any message using customary Indian music and keyboard illustration as a tool of encryption.

In the proposed method we relate two levels of encryption. First we renovate a usual text into traditional Indian music note using table 1. We then renovate the text into western music notes of a piano or a key board. While converting we use 1 for space between same word and 0 for space between two different words.

Table 1 provides the conversion of alphabets and numbers into Indian musical notes. Table 2 provides the conversion into western music notes.

Designing table 1 and 2 is the choice of the person sending the message. The alphabets from A – Z and numbers from 0 – 9 can be arranged in 36! Ways. For every alternative of these 36! ways we can assemble the music notes in 36! ways. Similarly table 2 can be designed in 7! methods and for each option of these 7! Ways the music notes can be arranged in 7! Ways. These two tables will be the key for encryption and decryption.[20]

Table 1: Conversion to Indian Musical Notes

Alphabet / Number	Music Conversion	Alphabet / Number	Music Conversion
A	SA	S	GASA
B	RE	T	SAMA
C	GA	U	REPA
D	MA	V	GADHA
E	PA	W	MANI
F	DHA	X	PASA
G	NI	Y	SAPA
H	SAGA	Z	NIMA
I	REMA	0	DHAGA
J	GAPA	1	PARE
K	MADHA	2	MASA
L	PANI	3	SASA
M	DHASA	4	RERE
N	SADHA	5	GAGA
O	NIPA	6	MAMA
P	DHAMA	7	PAPA
Q	PAGA	8	DHADHA

In table 1 we see that the first seven alphabets are allocated the fundamental music notes Sa, Re, Ga, Ma, Pa, Dha, Ni. The rest alphabets from H – Z and the numbers 0 – 9 are assigned a conversion which is a grouping of the seven music notes. This can be designed as per the first choice of the encoder and decoder.
For example the number 9 is assigned a conversion NINI in table 1. But as an alternative we could disperse any other amalgamation like MAPA, NIDHA (Note hat these are not used in the table). So designing the table is solely the selection of the encoder and decoder. This amplify the probable ways in which the table can be designed spaced out from the (36!)2 ways shown in the table 1.[20]

Table 1 is the main key for encryption of any message containing a string of alphabets and numbers.

Table: 2 Conversions to Western Musical Notes

Indian Music Note	Keyboard Notation
SA	C
RE	D
GA	E
MA	F
PA	G
DHA	A
NI	B

Space between two letters of same word	1
Space between two different words	0

Encryption Algorithm: by *M. Yamuna*1 , Krishna Pandey 2 , Nikhil Choudhary 3 et al.[20]*

Let S be the text to be encrypted

- Step 1 change S into Indian music note S1 using table 1.
- Step 2 change S2 into keyboard music note S2 using table 2.
- Step 3 Send S2 to the receiver

Decryption Algorithm:

- Step 1 From S2 obtain S1 using table 2.
- Step 2 From S1 generate S using table 1.

ILLUSTRATION

The message to be encoded is I LOVE MUSIC

After converting using table 1 we get S1 as

Word 1 REMA

Word 2 PANI NIPA GADHA PA

Word 3 DHASA REPA GASA REMA GA

So that string S1 is S1 REMA PANI NIPA GADHA PA DHASA REPA GASA REMA GA (seperated by space).

ISBN: 978-93-5407-648-0

S1 is again converted into keyboard notation S2 using table 2 as

S2 DF0GB1BG1EA1G0AC1DG1EC1DF1E

Note that here 0 correspond tos the freedom between words and 1 space between letters in the same word to facilitate encryption. Send DF0GB1BG1EA1G0AC1DG1EC1DF1E to the receiver.

Suppose the received message is AC1DG1EC1DF1E0FD1DG1DF1CA1G1F0AC1G

We know that 0 represents the space between words. So we recognize that there are three words in the note receive.

They are

Word 1 AC1DG1EC1DF1E

Word 2 FD1DG1DF1CA1G1F

Word 3 AC1G

In each word 1 represents the space between letters. Using table 2 we convert the words as

Word 1 DHASA REPA GASA REMA GA

Word 2 MARE REPA REMA SADHA PA MA

Word 3 DHASA PA

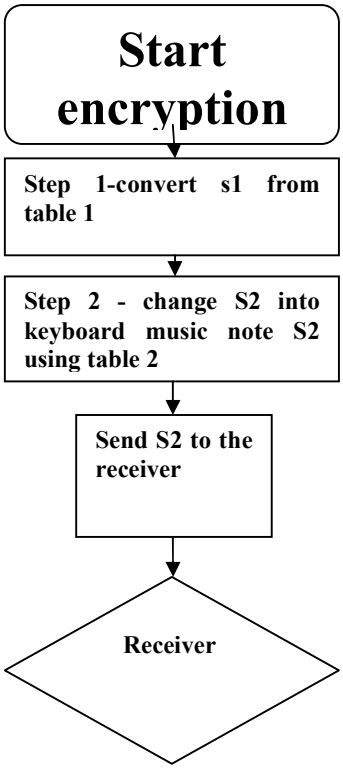
Now using table 1 the words are converted as

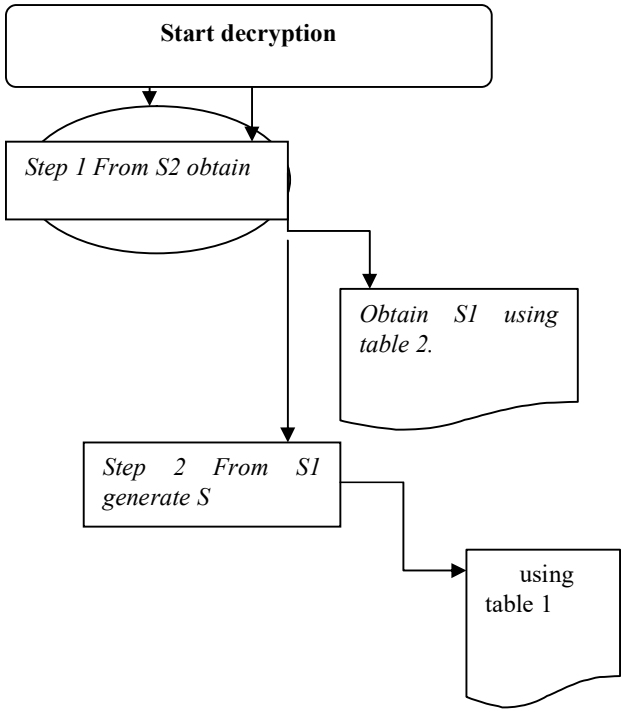
Word 1 MUSIC

Word 2 RUINED

Word 3 ME

So the decoded message is MUSIC RUINED ME.


Start encryption
Step 1-convert s1 from table 1
Step 2 - change S2 into keyboard music note S2 using table 2
Send S2 to the receiver
Receiver



5.2 By Using Music Sheet Cipher

Source code

dCode retains possession of the online 'Music Sheet Cipher' tool source code. Except explicit open source licence (indicated CC / Creative Commons / free), any algorithm, applet or snippet (converter, solver, encryption / decryption, encoding / decoding, ciphering / deciphering, translator), or any function (convert, solve, decrypt / encrypt, decipher / cipher, decode / encode, translate) written in any informatic language (PHP, Java, C#, Python, Javascript, Matlab, etc.).

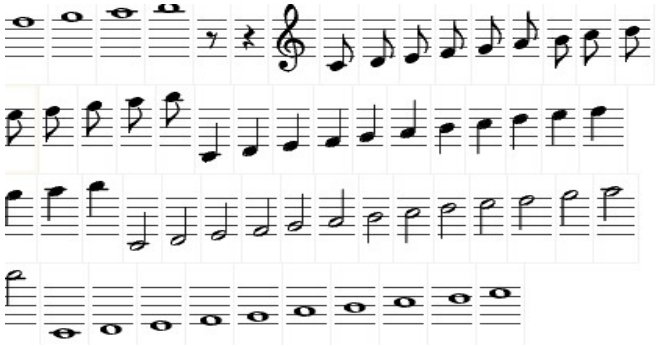
dCode is a toolkit website for decryption, ciphertexts, cheating at letter games, solve riddles, treasure hunts, etc. Opened in 2009, the site has grown steadily and improved, offering more and more tools and carried by its users, dCode has become a public site, free and open to all.

 ISBN: 978-93-5407-648-0

Figure 4- ***SYMBOLS FOR THE MUSIC SHEET***

How to encrypt using a music sheet?

Encryption uses 14 notes and eighth notes, quarter notes, half note and whole note, this is 4*14=56 symbols + 3 extras. There are many ways to encode letters with these 59 symbo

Example 1 : alphabet is composed of 14 eighth notes then the first 12 quarter notes : do1 = A, re1 = B, ... si1 = G, do2 = H, until sol2 = N then quarter notes do1 = O, etc. until fa2 = Z.

Example 2 : alphabet is composed of the first 13 eight notes then the 13 first quarter notes.

How to decrypt using a music sheet cipher?

The decryption of the Musical Sheet Cipher consists in the replacement of the 59 symbols (notes) by the characters of a defined alphabet.

- The ciphered message is composed of classical notes without musical value.
- The notation used does not necessarily matter, no more than the instruments or actually produced sound.
- The sheet can be printed without a key or other important detail for a musician.

Encryption

Plain text - practice makes man perfect

ABCDEFGHIJKLM-NOPQRSTUVWXYZ-
ABCDEFGHIJKLM-NOPQRSTUVWXYZ----

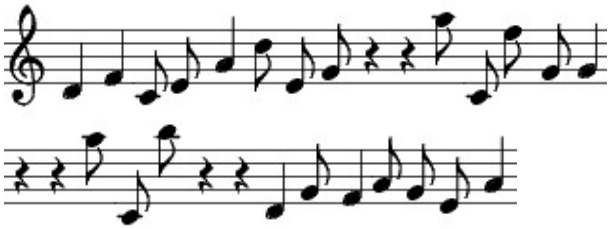



Figure 5 - Encypted sheet

Decryption

XNOHIVWYX

↑↓ ↑↓

<c>(A-Za-z0-6)</c>0LOgP

<c>(A-Z0-90-9)</c>-LO4P

<c>(0-9A-Z0-9)</c>--ASB

<c>(0-90-9A-Z)</c>Y-0E1

<c>(A-Za-z)</c> yLOeP

<c>(A-MN-Za-mn-z)</c> xLNeO

<c>(a-mn-zA-MN-Z)</c> XlnEo

<c>(A=♪Ré=♪D)</c> 9-JEK

5.3 Music Staff Notation

the reading is based on solfeggio. dCode can covert a staff into notes by translating the most common 14 notes and their variation sharp # and flat b.

Example: **DO**	**C**	**RE**	**D**	**MI**	**E**
FA	**F**	**SOL**	**G**	**LA**	**A**
SI	**B**				

Why a1 and a2?

In order to transcribe the two level of notes, the first level can be suffixed by 1 and the second by 2.

Why flat and sharp are not on the partition?

dCode has taken the liberty to simplify the writing of dieses and bemols, they are normally on the same level as their following note.

Music notes in alphabetical notation

C, D, E, F, G, A, B

A# A1 A2 A2b

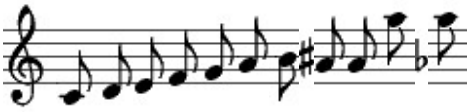



Figure 6- musical notes of western piano

Music notes in digit notation

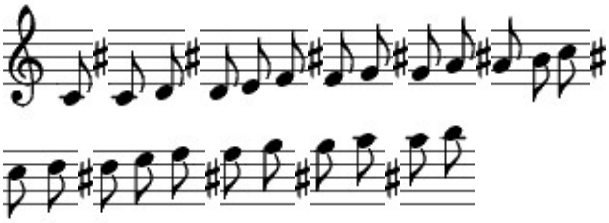
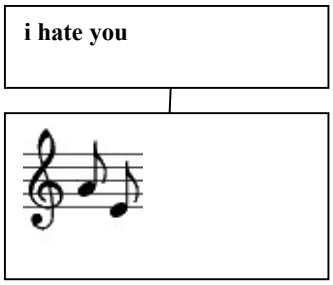
1 1.5 2 2.5 3 4 4.5 5 5.5 6 6.5 7 8 8.5 9 9.5 10 11 11.5 12 12.5 13 13.5 14

ISBN: 978-93-5407-648-0

Figure 7- Music notes in digit notation

Illustration



7. USING GUITAR CHORDS

In this approach, the sound of guitar chords is being used to encrypt and also the chord finder i.e. the sound recognizer is used for decrypting.

Algorithm is based on three steps –

1. First step: to allocate a guitar chord to every letter and symbol for each word in the text
2. Second step: to exchange the assigned chords into sound or perceptible format from texted format.
3. Third step: to adapt back the audio file by sound recognizer from audio to text format.

Using the following table 5 and Figure 8

As there are no E# (sharp) and B# (sharp) hence it is not used in the algorithm. Now for converting text we can use the table 5 and procedurally covert into musical files. For example: Text: ALL IS WELL.

Using table 1 we convert the text as follows:

TABLE 3

A	C major
L	A minor
I	G major
S	A#
W	G minor
E	E major
.	High hats

After converting this into an audio file, using step two listed before, we can send this file in mp3 format.

Decrypting Texts

- Receiving the audio file, the receiver can decrypt it with an accessible key for the conversion.
- A tool to listen the sound and make out which chord is played is required for this process
- . With sound recognizer the receiver generates following:
- C major- by back tracing table will get alphabet A, similarly

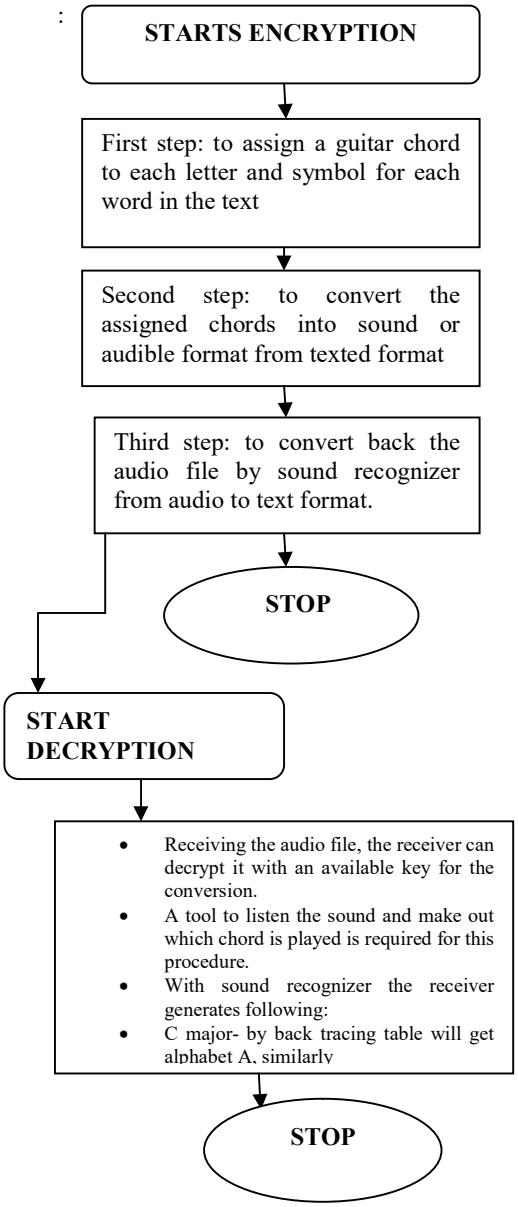
TABLE 4

A minor- L
G major- I
A# -S
G minor- A#
E major- W
High hats- .

TABLE 5

A	C major
B	C minor
C	D major
D	D minor
E	E major
F	E minor
G	F major
H	F minor
I	G major
J	G minor
K	A major
L	A minor
M	B major
N	B minor
O	C#
P	D#
Q	F#
R	G#
S	A#
T	C# minor
U	D# minor
V	F# minor
W	G# minor
X	A# minor
Y	C7 major
Z	C7 minor
0	D7 major
1	D7 minor
2	E7 major
3	E7 minor
4	F7 major
5	F7 minor
6	G7 major
7	G7 minor
8	A7 major
9	A7 minor
.	High hats
space	Kick drum
?	Crash
,	Snare

 ISBN: 978-93-5407-648-0


:
STARTS ENCRYPTION
First step: to assign a guitar chord to each letter and symbol for each word in the text
Second step: to convert the assigned chords into sound or audible format from texted format
Third step: to convert back the audio file by sound recognizer from audio to text format.
STOP
START DECRYPTION
Receiving the audio file, the receiver can decrypt it with an available key for the conversion.
A tool to listen the sound and make out which chord is played is required for this procedure.
With sound recognizer the receiver generates following:
C major- by back tracing table will get alphabet A, similarly
STOP

8. By Using Genetic algorithm

In the proposed system Genetic algorithm is being employed for Encrypting messages into musical notes. Genetic algorithms are evolutionary algorithms which use the concept of innate selection and genesis.It is used to explain explore problems when the search space is vast and also used for solving optimization problems. The necessary proposal behind using genetic algorithm is to generate an optimal musical sequence soothing to ears. Genetic algorithms have been used in field of music since ancient times. But the approach of looking towards it as a technique for generating a musical sequence is changed. In this paper the concept of cryptography combined with the Genetic Algorithm to encrypt messages into musical notes introduces the concept of Musical Cryptography. It is a traditional method being used to symbolize messages in the form of musical cryptograms. In this paper a new algorithm is being proposed for Encryption and Decryption rather than using the traditional methods and algorithms.

Encryption:
Since the Encrypted output would be a musical piece we need set of notes. In this scheme a set of western notes are being initialized and assigned to letters of plain text. Initial population is being generated by assigning set of notes. This gives us the initial population for the genetic algorithm. All possible combinations of notes initialized along with frequency values are are tested find which sequence produces more natural music. A probability matrix is being generated based on the standard sequence. This matrix would give us in sequence about what would be the probability of each note to occur after the previous note. Along with the probability matrix we necessitate one more table i.e the frequency table which contains detains about the the frequency values for each note along with a serial number assigns to each note as a primary key. Fitness value for each musical sequence is calculated based on the probability matrix. One with the highest fitness is selected as the encrypted output.Genesis rules are applied on it. Based on the rules we get the optimized output. This output is now in the form of musical notes. It is given to an note generation algorithm which takes the Musical notes and their corresponding frequency values as input. A sound would be played which is the final output.

Decryption:
In decryption the sound generated is taken as an input and based on the music the notes and their frequency values are retrieved from the database. The reverse process is applied to obtain the actual message / Plain text.

Other techniques for Encryption**:**

DES: DES is a asymmetric Key ciphering technique. DES is a block cipher, block size is 64 bits. DES uses either 56 bits or 128 bits. A single block of plaintext is transformed into ciphertext after passing through the following stages:

- An initial Permutation
- 16 rounds of a given function
- A 32-bit left-right swap
- A final permutation

The DES function is made up of P and S-boxes. P-boxes transpose bits and S-boxes substitute bits to generate a cipher. Since DES uses 56-bit key for encryption, 256 possible keys can be generated due to which brute force attack on such number of keys is impractical.Triple DES was introduced later to replace the original DES. It uses 3 individual keys with 56 bits.

AES: Advanced Encrytion Standards is a symmetric Key block cipher published by the NIST in December 2001.AES is a non Fiestal Structure. The key is developed into an array of forty-four 32 bit words.Four unlike stages are used,one of pernutation and three of substitution.For both encryption and decryption, the cipher begins with an AddRound stage, followed by nine rounds that each includes all four stages, followed by tenth round of three stages.Only the AddRound stage make use of the key.The AddRound stage is, in effect,a form of Vernam Cipher and by itself would not be formidable.Each stage is easily reversible.The decryption algorithm makes use of the expanded key in reverese order. Once it is recognized that all four stages are reversible, than its easy to verify that decryption can recover the plaintext. The final round of both encryption and decryption consists of only three stages.

RSA: RSA uses public-key for encryption. RSA is an asymmetric algorithm as it makes use of a pair of keys. Public key is used to encrypt the message and private key is used to decrypt it.RSA stands for Rivest, Shamir & Adleman intoduced in 1977 and it is best known & widely used public-key scheme. RSA makes use of an expression with exponentials.

- The algorithm for RSA is as follows:
- Select p, q where p and q both prime, p is not equal to q. Calculate n = p * q
- Calculate f(n) = (p - 1)(q - 1)
- Choose e such that 1 < e < f(n) such that e is co-prime
- Calculate d : d= e-1 (mod f(n))
- Public key PU = {e, n}
- Private key PR = {d, n}
- Encryption:
- Plaintext: M
- Ciphertext: C = M e mod n
- Decryption:
- Plaintext: M = Cd mod n.

ElGamal Algorithm: ElGamal cryptosystem is also called the Elliptic Curve Variant, is based on the Discrete Logarithm Problem. It is based on two factors one is choosing the large prime number p and next is choosing the generator element g.

Encryption:

C1= gk mod p

C2= p*yk mod p

Send the ciphertext C, consisting of the two separate values (C1, C2), sent together.

Decryption:

- In order to decrypt the ciphered text (C1, C2) using the private key x, following two steps are has to be taken:
- Compute the inverse of (C1)x modulo p, which is (C1)-x called the decryption factor.
- Obtain the plaintext by using the following formula:
- C2 X (C1)-x mod p= Plaintext

9.ANALYSIS

Cryptography attempt at changing over a secret message into a garbled book while, steganography targets concealing the furtive note inside a cover medium which could be a sound/text record. The proposed cycle is worried about renovateing a mystery instant message into a hear-able clasp which is itself the mystery being sent and subsequently is fairly connected to both the hypothesis of cryptography and steganography.

As clarified before, different mappings are potential for a given raga. Regardless of whether an assailant with some data of Carnatic music is fit to recognize the raga from a music cut, he/she won't have the option to unscramble it without knowing the arrangement of swara to plaintext planning. Accordingly ciphertext-just and man-in-the-center assaults can be kept away from.

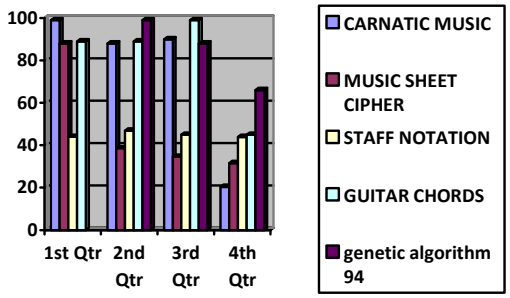


FIGURE 8- COMPARISION OF ALL ALGORITHMS

10. FUTURE SCOPE

- I will also be applying Braille alphabetic conversion to generate a new algorithm for musical cryptography.
- Further I will also be analyzing BETHOVEN"S TABLE and try extracting some fuzzy logic approach for cryptography.
- Musical symbols and musical notes have been used as the substitution cipher. The main goal of the musical cryptography is to

generate different musical cryptograms. I will also be analyzing some genetic algorithm for the same.

- I will also be using some more ragas to implement through musical cryptograms.

11. CONCLUSION

From the proposed method it might be construed that we can adequately use the melodic notes for encoding the messages. This technique of using notes makes it more difficult to perceive that there is some message concealed in it. Also, if it is recognized that there is a hidden message, the possibility of disentangling is less. As the third individual don't have key he/she can't disentangle it.. So using melodic language it is possible to encode the message. The stage and mixes expected to unscramble the message makes it nearly unfathomable gave the gatecrasher doesn't have the key.

We have used two stages of encryption one using traditional Indian music note and succeeding using our standard keyboard notes. It is complicated for whichever hacker to shatter the code except the conversion order into alphabets is known.

Also the 36 alpha numeric characters can be placed in a minimum of (36!)2 Ways and the 7 music notes in table can be arranged in (7!) 2 ways so that we can produce a table of our preference. This increases the security of the encrypted message and this collected works acts as a key for encryption and decryption. So the proposed encryption format is safe for encoding any message.

We were triumphant in creating a cipher table that produces consonant sounds, but the cipher itself does not have strapping security. Substitution ciphers are hardly ever used today because they are easy to split. This key distribution in this scenario presents a problem that has to be addressed through supplementary research.

9. ACKNOWLEDGEMENT

I WOULD LIKE TO THANKS MY FACULTY OF MY UNIVERSITY "AMITY UNIVERSITY JHARKHAND" PROF.TANNISHA KUNDU AND PROF. DR.POOJA JHA FOR GUIDING AND ALSO FOR LETTING ME KNOW ABOUT THIS CONFERENCE.AND ALSO I WOULD LIKE TO THANKS WHOLE CSE TEAM OF RIT FOR HELPING IN REGISTRATION.

12. REFERENCES

[1]. Sandip Dutta, Soubhik Chakraborty, N. C. Mahanti. "Novel Method of Hiding Message Using Musical Notes", 2010

[2] Chandan Kumar, Sandip Dutta, Soubhik Chakborty."ASymmetric Key Algorithm for Cryptography using Music",2013.

[3] Mohammed AbuTaha, MousaFarajallah, RadwanTahboub and Mohammad Odeh, "Survey Paper: Cryptography Is The Science Of Informatio Security," International Journal of Computer Science and Security (IJCSS), Volume (5): Issue (3): 2011.

[4] Marandi, Y.M.H., Sajedi, H. & Pirasteh, S. A novel method to musicalize shape and visualize music and a novel technique in music cryptography. Multimed Tools Appl (2020). https://doi.org/10.1007/s11042-020-09962-8

[5] Weiß C, Müller M (2015) Tonal complexity features for style classification of classical music. 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE

[6] Tucker GM, Jones AV, Latham A (2011) The Oxford companion to music. Oxford University Press, Oxford

[7] Rodrıguez-González S, Pérez-Lancho B (2018) Modeling a Synaesthete System to Generate a Tonal Melody from a Color Distribution. International Joint Conference SOCO'18-CISIS'18-ICEUTE'18: San Sebastián, Spain, June 6–8, 2018 Proceedings. Vol. 771. Springer

[8] Lamaute N, et al (2016) A substitution cipher for musical cryptography. In: Proceedings of Student-Faculty Research Day, CSIS, Pace University

[9] Piano Keyboard Guide, Piano Keyboard. 2016. (No subject)

[10] Desmedt Y., Hou S., Quisquater J.J. (1998) Audio and Optical Cryptography. In: Ohta K., Pei D. (eds) Advances in Cryptology — ASIACRYPT'98. ASIACRYPT 1998. Lecture Notes in Computer Science, vol 1514. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-49649-1_31

[11] M. Maity, "A Modified Version of Polybius Cipher Using Magic Square and Western Music Notes,International Journal for Technological Research in Engineering, vol. 1 no.10, (2014)

[12] Moumita Maity. "A MODIFIED VERSION OF POLYBIUS CIPHER USING MAGIC SQUARE AND WESTERN MUSIC NOTES" International Journal For Technological Research In Engineering Volume 1, Issue 10, June-2014

[13] W. Stallings, Cryptography and Network Security

Principles and Practices, Prentice Hall, 2011

[14] N. J. Thorwirth, P. Horvatic, R. Weis and Jian Zhao, "Security methods for MP3 music delivery," Conference Record of the Thirty-Fourth Asilomar Conference on Signals, Systems and Computers (Cat. No.00CH37154), Pacific Grove, CA, USA, 2000, pp. 1831-1835 vol.2, doi: 10.1109/ACSSC.2000.911304.

[15] Alimomeni, M., Safavi-Naini, R.: Human assisted randomness generation using video games. IACR Cryptol. ePrint Archive 2014, 45 (2014)

[16] Tsai, J.M., Chen, I.T., Tzeng, J.: Random number generated from white noise of webcam. In: Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. IIH-MSP'09, pp. 214–217. IEEE (2009)

[17] . Lacy, J. H. Snyder and D. P. Maher, "Music on the Internet and the intellectual property protection problem," ISIE '97 Proceeding of the IEEE International Symposium on Industrial Electronics, Guimaraes, Portugal, 1997, pp. SS77-SS83 vol.1, doi: 10.1109/ISIE.1997.651739.

[18] P. Z. Onufryk and J. H. Snyder, "Consumer Devices for Networked Audio", Proceedings of the 1997 IEEE International Symposium on Industrial Electronics.

[19] IS 13818-7 (MPEG-2 Advanced Audio Coding, AAC), M. Bosi, K. Brandenburg, S. Quackenbush, M. Dietz, J. Johnston, J. Herre, H. Fuchs, Y. Oikawa, K. Akagiri, M. Coleman, M. Iwadare, C. Lueck, U. Gbur, B. Teichmann.

[20] M. Yamuna , Krishna Pandey , Nikhil Choudhary "CRYPTOGRAPHY USING MUSIC NOTES" Volume 4, No. 4, April 2013 Journal of Global Research in Computer Science

[21] C. Kumar, S. Dutta and S. Chakborty, "Musical cryptography using genetic algorithm," 2014 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2014], Nagercoil, 2014, pp. 1742-1747, doi: 10.1109/ICCPCT.2014.7054851.

[22] Norissa Lamaute, Alexa Piccoli, Li-Chiou Chen, and Andreea Cotoranu "A Substitution Cipher for Musical Cryptography" Proceedings of Student-Faculty Research Day, CSIS, Pace University, May 6th, 2016

[23] J. McCormac, "European Scrambling Systems Circuits Tactics and Techniques" in The Black Book, Waterford University Press, vol. 4, 1994.

[24] Wikipedia contributors. (2020, July 22). Musical cryptogram. In Wikipedia, The Free Encyclopedia. Retrieved 02:49, November 21, 2020, from https://en.wikipedia.org/w/index.php?title=Musical_cryptogram&oldid=968933237